



County of Los Angeles
CHIEF ADMINISTRATIVE OFFICE

713 KENNETH HAHN HALL OF ADMINISTRATION • LOS ANGELES, CALIFORNIA 90012
(213) 974-1101
<http://cao.co.la.ca.us>

DAVID E. JANSSEN
Chief Administrative Officer

July 9, 2004

Supervisor Don Knabe, Chair
Supervisor Gloria Molina
Supervisor Yvonne Braithwaite Burke
Supervisor Zev Yaroslavsky
Supervisor Michael D. Antonovich

Board of Supervisors
GLORIA MOLINA
First District

YVONNE B. BURKE
Second District

ZEV YAROSLAVSKY
Third District

DON KNABE
Fourth District

MICHAEL D. ANTONOVICH
Fifth District

Dear Supervisors:

**GREEN AND SHINEE LETTER OF JUNE 28, 2004
RE: CHIEF INFORMATION OFFICER (CIO)
INFORMATION TECHNOLOGY SECURITY POLICIES
JULY 13, 2004, AGENDA ITEM NO. 10**

My staff in conjunction with CIO staff has reviewed the subject letter. In response to the concerns of Mr. Shinee and the Coalition of County Unions (CCU), departments with employees represented by the CCU were surveyed by the CIO to determine if Information Technology Security policies were currently in place. Each department had either an existing policy and/or an Acceptable Internet Use Agreement.

Attached are our responses to Mr. Shinee. If you have any questions, please call me at (213) 974-1101, or your staff may contact James Adams of my staff at (213) 974-2404.

Sincerely,

A handwritten signature in black ink, appearing to read "David E. Janssen", is written over a printed name and title.

DAVID E. JANSSEN
Chief Administrative Officer

DEJ:JA
PDC:mj

c: Jon Fullinwider, CIO

Attachments

BOS Ltr. CCU-Shinee



County of Los Angeles
CHIEF ADMINISTRATIVE OFFICE

713 KENNETH HAHN HALL OF ADMINISTRATION • LOS ANGELES, CALIFORNIA 90012
(213) 974-1101
<http://cao.co.la.ca.us>

DAVID E. JANSSEN
Chief Administrative Officer

July 8, 2004

Mr. Richard Shinee, Attorneys at Law
A Professional Corporation
16055 Ventura Blvd, Suite 1000
Encino, California 91436-2680

Dear Mr. Shinee:

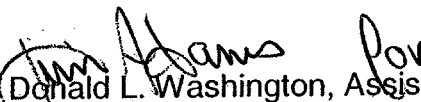
**JUNE 29, 2004, BOARD AGENDA ITEM NO. 18
CHIEF INFORMATION OFFICER (CIO)
(INFORMATION TECHNOLOGY SECURITY POLICY)**

Attached are the Department of Mental Health Information Technology Security policies and Acceptable Internet Use Agreement.

The Chief Information Officer has surveyed County departments with employees represented by the Coalition of County Unions and determined that each department has an Information Technology Security Policy and/or an Acceptable Internet Use Agreement.

Sincerely,

DAVID E. JANSSEN
Chief Administrative Officer


Donald L. Washington, Assistant Division Chief
Employee Relations Division

Attachments

DEJ:JA
DLW:mj

c: Paul Roller, Chair, Coalition of County Unions
Jon Fullinwider, Chief Information Officer

Shinee Ltr.

Board of Supervisors
GLORIA MOLINA
First District

YVONNE B. BURKE
Second District

ZEV YAROSLAVSKY
Third District

DON KNABE
Fourth District

MICHAEL D. ANTONOVICH
Fifth District



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|--------------------------|------------------------------------|-------------------------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 09/15/03 | PAGE 1 of 10 |
| APPROVED BY: Director | SUPERSEDES 302.14 | ORIGINAL ISSUE DATE 04/14/03 | DISTRIBUTION LEVEL(S) 2 |

PURPOSE

- 1.1 This policy governs the use of Department of Mental Health (DMH) information technology resources. It includes rules in compliance with the **Health Insurance Portability and Accountability Act (HPAA) Standards for Privacy of Individually Identifiable Health Information**. (45 CFR Parts 160 and 164)
- 1.2 This policy communicates to all DMH employees, volunteers, contractors and consultants their responsibility for acceptable use of DMH information technology resources.
- 1.3 The term "user" as used throughout this policy/procedure document is used broadly and refers to paid employees, students, volunteers, interns, consultants, contractors and any other persons who represent the Department in the course of their work duties.
- 1.4 By logging on to the computer system, the user acknowledges that he/she understands and accepts the terms and conditions of this policy.

POLICY

- 2.1 The scope of this policy includes all aspects of the networked computing environment in DMH, whether or not the equipment is connected to the Departmental network (hereafter referred to as "DMH Network"). This includes all desktop and notebook computers as well as other information devices such as PDA's and wireless networks.
- 2.2 The DMH Network includes all servers and workstations connected to it, via direct or remote connection. By extension and for the purpose of this policy, it also includes portions of LANet and other County Information systems.
- 2.3 Where it comes into conflict with other existing departmental policies in the area of computing, this document shall take precedence (unless the other policies contain higher levels of security and control requirement, in which case the higher-level requirements supersede), until such time when the conflicting policies are reconciled.
- 2.4 The DMH Chief Information Office, Human Resources Bureau, Administrative Support Bureau, Contract Administration and managers of all units shall carry out the enforcement of this policy where appropriate.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|----------------------|-------------------------------|-----------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 2 of 10 |
|---|----------------------|-------------------------------|-----------------|

- 2.5 Failure to comply with this policy, in whole or in part, if grounds for disciplinary actions, up to and including discharge.

ADMINISTRATIVE CONTROL

- 3.1 The CIO Bureau's Information Technology Security Officer (ITSO) is the designated person with functional responsibilities for DMH Network security and control.
- 3.2 The ITSO is responsible to the DMH Chief Information Officer.
- 3.3 Training in areas of computing and security policies shall be provided to all users in appropriate forms (e.g., training sessions, manuals and other documents).
- 3.4 This policy shall be added to the list of policies each used must review and to be so certified on the Department's Annual Policy Certification form.
- 3.5 Certain projects/programs within DMH, because of their sensitive nature, might require a higher level of security than this document specifies. Users may be required to sign other documents when performing tasks that demand higher levels of security.
- 3.6 All managers are responsible for enforcing this policy in their respective units. Managers are also responsible to review the security compliance in their respective units at least quarterly.

DATA SECURITY

4.1 DATA CLASSIFICATION

- 4.1.1 Protected Health Information (PHI) Protected Health Information (PHI) is defined as any information, alone or in combination that allows a mental health client to be uniquely identified. PHI is accessible only to specifically authorized users.
- 4.1.2 Internal Data Internal data is confidential information that does not contain PHI. Only authorized DMH and contract agency users may access internal data.
- 4.1.3 Public Data Public Data is information that can be accessed by the general public.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|----------------------|-------------------------------|-----------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 3 of 10 |
|---|----------------------|-------------------------------|-----------------|

4.2.1 Network Storage

- 4.2.1.1 All users of networked workstations shall store PHI data in network folders that the CIO Bureau designates. This may include the user's electronic personal home folder.
- 4.2.1.2 The network staff shall backup the network servers and data residing on the designated network directory daily.

4.2.2 Local Storage

- 4.2.2.1 PHI shall not be stored locally (i.e., the hard drive of a desktop or notebook computer). Printing of hard copy of PHI requires approval of the user's manager. The hard copy shall be securely stored.
- 4.2.2.2 PHI data shall not be stored on removable devices (e.g., diskette, ZIP or JAZ cartridges, CDROM).
- 4.2.2.3 In the instance where PHI must be stored on notebook computers while not connected to the DMH Network, the hard drive on such computers shall be encrypted.

PHYSICAL SECURITY

5.1 SERVER

- 5.1.1 All server equipment shall be located in a secure area, inside a secured County building. Access to this area shall be controlled.
- 5.1.2 Any unauthorized access to the server area shall be reported to the ITSO>
- 5.1.3 Transport of any equipment in or out of the server area required prior approval of the CIO Bureau's Network Manager.

5.2 OTHER NETWORK EQUIPMENT

- 5.2.1 All routers, switches and storage devices shall be located in a secured area, or in locked cabinets, inside a secured County building. Only authorized personnel may have access to these areas/cabinets.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|----------------------|-------------------------------|-----------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 4 of 10 |
|---|----------------------|-------------------------------|-----------------|

5.3 WORKSTATIONS

- 5.3.1 Workstations are defined as all desktop and notebook computers and other data devices, whether connected to the DMH Network or not.
- 5.3.2 All workstations and related components (e.g., monitor, printer, scanner, external storage devices, etc.) shall be secured.
- 5.3.3 Computer equipment casing shall not be opened; staff from the DMH CIO Bureau must perform hardware repairs and upgrades.
- 5.3.4 Personal equipment (including computers and peripherals) are not permitted on the DMH Network.

LOGICAL SECURITY

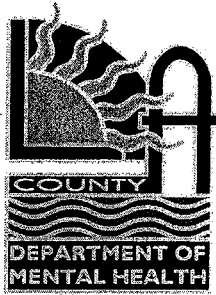
6.1 NETWORK SECURITY

6.1.1 Network Access

- 6.1.1.1 Network Access Authorization Access to network resources must be specifically requested and granted based on the user's business need.
- 6.1.1.2 Procedure for Requesting Network Access Persons wishing network access must make their request by submitting a *Network Access Request Form* (Attachment I). A manager at the level of Program Head or Division Chief must sign the form.

6.1.2 User Passwords

- 6.1.2.1 Network Password A user's network password allows the user to access predefined network resources such as the user's specific data director on the server. In addition to ensuring authorized access, the use of a network password creates a method for audit. Each user is responsible for any activity carried out under his/her credential (User ID and password). To ensure accountability, individual users shall not share their network passwords with anyone (including the user's supervisor).
- 6.1.3 Other Passwords Applications, both commercial and those developed in-house, might provide password protection to specific resources or data. Users shall treat such passwords the same as the Network Password.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|----------------------|-------------------------------|-----------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 5 of 10 |
|---|----------------------|-------------------------------|-----------------|

6.1.4 Account Policy The DMH Network account policy is implemented via the Microsoft Windows 2000 operating system. It is defined as follows:

- 6.1.4.1 Maximum Password Age: 30 days
- 6.1.4.2 Minimum Password Age: 1 day
- 6.1.4.3 User ID: User's first initial and full last name (and, when necessary, middle initial). Official name on record with Human Resources shall be used to determine the User ID.
- 6.1.4.4 Minimum Password Length: 8 characters
- 6.1.4.5 Complexity required (must meet three of the following four conditions: uppercase letter, lowercase letter, number, punctuation mark).
- 6.1.4.6 System remembers last six (6) passwords.
- 6.1.4.7 Account lockout after three (3) bad attempts.
- 6.1.4.8 After the lockout, user must contact the Help Desk to have it reset.
- 6.1.4.9 Connection will expire after logon house expire. Logon hours to be based on need.

6.1.5 Remote Access Remote access to any DMH information system resources must be via CIO approved channels.

6.1.6 Control and Change Managers shall use the *Network Access Request Form* for addition of users, deletion of users, transfer of users, changing users' level of access and requesting data folder creation/access.

E-MAIL USAGE

7.1 Authorization

7.1.1 E-mail services are provided to all authorized DMH staff. Authorization for a person to have an e-mail account is granted along with the user's network access.

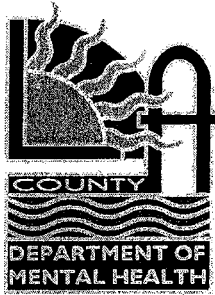
7.1.2 E-mail services are provided for County-related business needs only.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|----------------------|-------------------------------|-----------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 6 of 10 |
|---|----------------------|-------------------------------|-----------------|

- 7.1.3 All users are responsible for the regular maintenance of their e-mail account, which includes purging and archiving e-mail messages to ensure the mailbox has enough space to receive messages.
- 7.2 E-mail messages and their attachments are the property of the Department and not private communications, whether created or received, and may be subject to review by the Department at any time.
- 7.3 User may use e-mail to communicate with users in other entities so long as the communication meets professional standards of conduct and when such communication is related to legitimate business activities.
- 7.4 All users are responsible to report observed inappropriate use of e-mail (as defined in this policy).
- 7.5 E-mail communication may not contain any Protected Health Information (PHI) as defined in Section 4.1.1 of this policy.
- 7.6 Upon request of the DMH Chief Information Officer or Chief Deputy Director, DMH may access any user's electronic mail.
- 7.6.1 The above notwithstanding, the Department will **not** routinely monitor individual user's e-mail and will take reasonable precautions to protect the privacy of e-mail. Accordingly, supervisory and management staff may access an authorized user's e-mail when DMH operations require it (for example, when the employee is on vacation or otherwise absent from work).
- 7.6.2 Technical staff from the CIO Bureau may access a user's e-mail to diagnose and resolve technical problems involving system hardware, software or communications.
- 7.6.3 Except as noted above, a staff member is prohibited from accessing another user's e-mail without his/her permission.
- 7.6.4 E-mail messages may be retrieved by the Department (including messages deleted by users). Such messages may be used in disciplinary actions. The contents of e-mail will not be accessed or disclosed other than for investigative or security purposes, or as required by law.
- 7.7 Employees **may not** use e-mail for transmission of the following information:
- 7.7.1 Discrimination on the basis of race, creed, color, gender, religion, disability or sexual preference.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|------------------------------|--|-------------------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 7 of 10 |
|---|------------------------------|--|-------------------------|

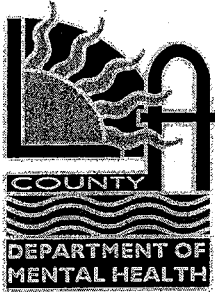
- 7.7.2 Sexual or other forms of harassment or threats. This includes the display or transmission of sexually explicit images and text as well as the use of racial epithets or ethnic slurs.
- 7.7.3 Copyright infringement.
- 7.7.4 Personal political or religious beliefs.
- 7.7.5 Person business interests, including any activities such as sales, consulting for pay, moonlighting, etc.
- 7.7.6 Anonymous e-mail, or e-mail which impersonates or claims to be another individual.
- 7.7.7 Chain letters.
- 7.7.8 Spamming (e-mail to large numbers of people that contain unwanted solicitations or information).
- 7.7.9 Any messages or attachments that can adversely affect network performance (because of large size, etc.). Often it is better to distribute such information via the DMH Intranet or a network folder. Users who are uncertain about whether particular information should be distributed by e-mail should contact the Help Desk (213-351-2937).
- 7.7.10 Obscene language.
- 7.7.11 Virus alert. Users who suspect an e-mail contains a virus should contact the Help Desk (213-351-2937). The only individuals who are authorized to broadcast warnings about viruses to the rest of the Department are Executive Staff or Network staff.
- 7.7.12 Any other information that would jeopardize the legitimate interests of the Department.
- 7.7.13 Any unlawful or malicious activity.
- 7.8 To access e-mail, a user shall supply his/her network credential (User ID and password) either as part of the logon process to the DMH network or to OWA (Outlook Web Access).
- 7.9 In order to access DMH e-mail outside of the Los Angeles County network, a user needs a SecureID card.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|----------------------|-------------------------------|-----------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 8 of 10 |
|---|----------------------|-------------------------------|-----------------|

- 7.10 The content and maintenance of a user's electronic mailbox are the user's responsibility. The content and maintenance of a user's disk storage area are the user's responsibility. All users must regularly purge or archive outdated messages. All users must make sure their mailboxes have space to receive messages.
- 7.11 Directories of employee e-mail addresses shall not be made available for public access.
- 7.12 DMH may deem certain e-mail messages and/or their attachments business records. Such messages and attachments shall be retained as required by the Department's record retention policies.
- 7.12.1 Users shall retain all such messages and attachments, either as paper records or electronic file copies, in an existing filing system **outside the e-mail system** for as long as operational, legal, audit, research or other requirements dictate.
- 7.12.2 Users shall dispose of records in the e-mail system only after they have been filed in a record keeping system.
- 7.13 Protection Against Computer Viruses
- 7.13.1 Users shall not open e-mail messages, and particularly any attachment inside messages, if they suspect a virus might be present. Contact the Help Desk (213-351-2937) for directions.
- 7.13.2 CIO Bureau staff will make every attempt to notify all users of any viruses or worms that have infected e-mail messages. Upon such notification, all users shall completely delete the messages identified in the notification. In Microsoft Outlook, deleting completely requires deleting them from the Deleted Items folder as well as from the Inbox.
- 7.13.3 If you suspect an e-mail contains a virus, do not attempt to send out an alert. Instead, contact the Help Desk (213-351-2937). The only individuals who are to broadcast warnings about viruses to the rest of the Department are Executive Staff or Network staff.
- 7.14 Investigation of Suspected or Demonstrated Inappropriate E-Mail Usage
- 7.14.1 In appropriate e-mail usage by a user reported to (1) the Program Head or Manager at that departmental facility or division or, (2) a District Chief or Deputy Director shall be investigated promptly. The District Chief, Division Chief or Deputy Director shall first contact the CIO Data Security Unit. Together, they may take either or both of the following actions as appropriate:



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|------------------------------|--|-------------------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 9 of 10 |
|---|------------------------------|--|-------------------------|

- 7.14.1.1 Ask the employee how this e-mail message is related to Department business.
- 7.14.1.2 Review the e-mail message(s) and attachments involved.
- 7.14.2 If the investigation does not substantiate the report of inappropriate e-mail usage, the Program Head, District chief or Deputy Director shall stop the investigation immediately, advise the employee and take no further action.
- 7.14.3 If the Program Head, District chief or Deputy Director deems the e-mail message to be inappropriate for any reason, the Deputy Director shall check with the DMH Chief Information Officer to ascertain if there are/were any other known e-mail offenses by this employee.
 - 7.14.3.1 Disciplinary actions, if any, will be in accordance with relevant County regulations and civil service regulations.
 - 7.14.3.2 If the District Chief or Deputy Director determines that the employee's e-mail access privileges are to be suspended or revoked, the District Chief or Deputy Director shall promptly notify the DMH Chief Information Officer of such determination.
- 7.15 The DMH Chief Information Officer shall suspend/revoke e-mail access immediately upon being notified of the determination by the employee's District Chief or Deputy Director. The e-mail account will remain closed until the matter is resolved.

COMMERCIAL SOFTWARE

8.1 Standard

- 8.1.1 The DMH approved list of commercial application software is shown in the Los Angeles County Department of Mental Health "Application Software Standard" (Attachment II).
- 8.1.2 The installation of any other software requires the approval of the ITSO. Users or units must submit a written request with justification to the CIO Bureau.
- 8.13 If non-standard software interferes with network security or the functions of the operating system, standard software or any hardware component, the non-standard software will be removed.
- 8.14 Instant Messaging and peer-to-peer file sharing software are strictly prohibited.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

| | | | |
|---|----------------------|-------------------------------|------------------|
| SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE | POLICY NO. 302.14 | EFFECTIVE DATE 10/01/03 | PAGE 10 of 10 |
|---|----------------------|-------------------------------|------------------|

- 8.15 Any other software that bypasses the DMH and Los Angeles County network security perimeter control without specific authorization is strictly prohibited.

8.2 Copyright Compliance

- 8.2.1 DMH holds license agreements with makers of standard software. To comply with the license requirements, only authorized staff from the CIO Bureau are allowed to perform installations or upgrades.
- 8.2.2 Users of non-standard software (see Section 8.1) are responsible for copyright compliance.
- 8.2.3 Unauthorized copying and installation of any software are violations of Federal law. Removal or moving of software might be a violation of the license agreement.
- 8.2.4 Personal copies of software shall not be installed on any County computer.

8.3 Application Software Developed by DMH

- 8.3.1 All software developed by DMH, whether internally or by contracted entities is considered to be the property of DMH.
- 8.3.2 Software development must follow standard industry guidelines.
- 8.3.3 All software, prior to being put into production, requires review and approval by the ITSO.

AUTHORITY

Auditor-Controller Internal Control Certification Program (ICCP) Requirements, 1999

ATTACHMENTS

Attachment I Network Access Request Form
Attachment II Application Software Standard.

REVIEW DATE

This policy shall be reviewed on or before November 15, 2004 and annually thereafter.

**COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE AND
CONFIDENTIALITY OF
COUNTY'S INFORMATION TECHNOLOGY ASSETS,
COMPUTERS, NETWORKS, SYSTEMS AND DATA**

As a Los Angeles County employee, contractor, vendor or other authorized user of County Information Technology (IT) assets including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT assets for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As a user of County's IT assets, I agree to the following:

1. Computer crimes: I am aware of California Penal Code 502(c) - Comprehensive Computer Data Access and Fraud Act (attached). I will immediately report any suspected computer misuse or crimes to my Management.
2. Security access controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's, etc.) or passwords.
3. Approved business purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.
4. Confidentiality: I will not access or disclose any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.
5. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any County computer, network, system or data. I will install and maintain computer virus detection and eradication software on my personal computer, servers and other computing devices I am responsible for.
6. Offensive materials: I will not access or send any offensive materials, e.g., pornographic, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.
7. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services are unfiltered and in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.
8. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will maintain and use proper business etiquette when communicating over e-mail systems.
9. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.
10. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, cancellation of contracts or both civil and criminal penalties.

**AGREEMENT FOR ACCEPTABLE USE AND
CONFIDENTIALITY OF
COUNTY'S INFORMATION TECHNOLOGY ASSETS,
COMPUTERS, NETWORKS, SYSTEMS AND DATA**

**CALIFORNIA PENAL CODE 502(c) -
"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"**

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website www.leginfo.ca.gov/.

502.(c) Any person who commits any of the following acts is guilty of a public offense:

- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.
- (2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

Employee's Name

Employee's Signature

Date

Manager's Name

Manager's Signature

Date

DD:dd
policies
datasecc



LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH
550 S. VERMONT AVENUE, LOS ANGELES,
CALIFORNIA 90020

SECURITY INCIDENT REPORT

Form & Procedures

(SIR)

PROCEDURES

1. A Security Incident Report (SIR) must be filed whenever any of the following occurs on **DMH property** or directly affects **DMH property or employees**:

- ◆ Abusive or threatening language or behavior toward another employee, a supervisor, or any other person on DMH premises;
- ◆ Unauthorized entrance to County premises during non-scheduled working hours or entrance into unauthorized areas during regular working hours;
- ◆ Any threats or acts of arson, robbery, rape, vandalism, etc. occurring on DMH property;
- ◆ Any incident that places ON-DUTY County employees at risk of becoming a victim of violence and/or crime while on County property or places County property at risk including incidents which require action by law enforcement, County safety police or security guards (whether they were summoned or not);
- ◆ Read the Code Reference Information sheet for a list of all the incidents you can report using this form!

2. The SIR may be completed by the following individuals: a person directly involved in the incident, the on-site manager or the facility safety officer.

- The back of the SIR form contains the Code Reference Information.

3. Once the SIR is completed:

- (a) Write a brief memo describing the circumstances of the incident.
- (b) If the situation requires immediate action, call Barbara Cienfuegos after the fax has been submitted to advise her of the situation.
- (d) Fax the package no later than the end of business, on the day following the incident to each of the following:
 - (1) On-site Safety Officer or his/her designee

- (2) Barbara Cienfuegos, LCSW
Departmental Health & Safety Officer
550 South Vermont Avenue, 11th Floor
FAX (213) 427-6162
Email bcienfuegos@dmh.co.la.ca.us

- (3) **Send the SIR only ... do not send the memo.**
Office of Security Management
500 West Temple Street, Room 785
Los Angeles, California 90012
FAX to (213) 613 – 0744

4. Employee Threats

- (a) You must receive confirmation from Barbara Cienfuegos or her designee that she has received your SIR by a telephone call, email message or fax by the end of the business day.
- (b) Serious Threats - You must receive confirmation of your fax within two hours.
 - (1) Immediately follow up with a phone call to Barbara Cienfuegos.
 - (2) If you cannot contact Barbara Cienfuegos, then you must contact Linda Boyd (213) 738 – 4924 or Tony Beliz (213) 738 – 4924.

If you have any questions, please call Barbara Cienfuegos at (213) 738-4919.

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

RIO HONDO MENTAL HEALTH

SAMPLE

December 1, 2001

TO: Barbara Cienfuegos, LCSW
Health & Safety Officer

FROM: Mary Sample
Clinic Manager

SUBJECT: BURGLARY / RIO HONDO MENTAL HEALTH

On March 3, 1998, at 1:30 a.m., Mr. Mike Nelson was called out to Rio Hondo Mental Health by the Los Angeles Safety Police Central Office. Officer Armando Morales advised him that a window had been broken and suspect(s) had entered the building. First response was Cerritos Police who waited for and surveyed the interior (with a police dog) with Safety Police. Mr. Nelson and Officer Morales walked through the first floor to see if anything was missing. Nothing was missing. The Los Angeles County Safety Officer filed a report.

Your memo must answer the following seven questions:

1. **What happened?**
2. **When did this happen?**
3. **Where?**
4. **To Whom?**
5. **How did it happen?**
6. **Why did it happen?**
7. **What are your recommendations to "fix" the problem.**

BC

Attachment

c: Your Boss

OFFICE OF SECURITY MANAGEMENT/CAO

SECURITY INCIDENT REPORT

This report should be completed by the person reporting or involved in the incident, the building manager or his/her designee not later than the end of the business day following the incident. The report shall be delivered to:

- a) The Office of Security Management, 785 Kenneth Hahn Hall of Administration, 500 W. Temple Street, Los Angeles, CA 90012, or sent via FAX to (213) 613-0848 and,
- b) Barbara Cienfuegos, DMH Safety Officer. FAX (213) 427-6162

- **You must receive confirmation of your fax by the end of the business day.**
Read the procedures to find the steps to follow if you not receive a confirmation.

For this report, a SECURITY INCIDENT is defined as:

- An incident placing a person or property at risk that requires action by law enforcement authorities, County safety police or security guards at a County facility whether they were summoned or not. **OR**
- An incident placing a person or property at risk involving an ON-DUTY County employee (including lunch periods) while on County property. This classification includes parking facilities, or while walking to or from an off-site parking facility to start or end a work day. **OR**
- An incident of a suspicious or unusual nature on County property that places people or property at risk.

DATE OCCURRED _____ DAY OF WEEK _____ TIME _____

COUNTY DEPARTMENT REPORTING INCIDENT: **MENTAL HEALTH**

ADDRESS OF INCIDENT: _____

Is the suspect a County employee? Yes() No()

Is this incident gang related? Yes() No()

Was an arrest made? Yes() No()

Charge _____

The law enforcement agency that handled the incident: (Circle appropriate number)

| | <u>Department</u> | <u>Report Number</u> |
|----|-----------------------------|----------------------|
| 1. | L.A. County Sheriff's Dept. | _____ |
| 2. | L.A. Police Dept. | _____ |
| 3. | Local Police Dept. | _____ |
| 4. | L.A. County Safety Police | _____ |
| 5. | Contract Security Co. | _____ |
| 6. | None | _____ |

CODE FOR TYPE OF INCIDENT REPORTED: _____

(i.e., A-1 = Burglary of a County building, see reverse side of this form)

REPORTED BY: _____ day phone _____

APPROVED BY: _____ day phone _____

CODE REFERENCE SHEET FOR SECURITY INCIDENT REPORTS

A. Burglary: Entering a closed building or a locked vehicle with the intent to commit a theft.

1. Burglary of a County building (459 P.C.)
2. Burglary of a County vehicle (459 P.C.)
3. Burglary of a private vehicle (459 P.C.)
4. Burglary alarm no evidence of crime

B. Robbery: The taking of property from a person by force or fear.

1. Robbery of a County facility or employees performing their job (211 P.C.)
2. Robbery of a person, including employees, not performing their job (211 P.C.)

C. Arson: The intentional setting fire to any object. It is not necessary to destroy the object the mere charring is sufficient for arson.

1. Arson of a County building (447 P.C.)
2. Arson of a County vehicle (447 P.C.)
3. Arson of private property (including vehicles) (447 P.C.)

D. Rape: Forced sexual intercourse with the opposite sex.

1. Rape of a County employee (261 P.C.)
2. Rape of other than a County employee (261 P.C.)
3. Other sex related incident

E. Assault: The physical battering of another person.

1. Assault with a weapon (245 P.C.)
2. Assault no weapon, but requiring hospitalization of the victim (245 P.C.)
3. Assault with only minor injuries and no weapon was used (242 P.C.)

F. Theft of or from vehicle:

1. Theft of a County vehicle (487.3 P.C.)
2. Theft of a private vehicle (487.3 P.C.)
3. Theft from a County vehicle - no forced entry (488/487 P.C.)
4. Theft from a private vehicle - no forced entry (488/487 P.C.)

G. Theft not involving a vehicle:

1. Theft of County property valued under \$400 (488 P.C.)
2. Theft of County property valued over \$400 (487 P.C.)
3. Theft of private property (excluding vehicles) (488/487 P.C.)

H. Disturbances: No actual crime need to be committed. The disruption of routine business constitutes a disturbance.

1. Disturbance of a County employee or facility (415 P.C.)
2. Disturbance created by a County employee and/or their spouse involving a "domestic issue"
3. Disturbance not involving County employees
4. Threats (verbal or written) to a County employee
5. Refusal to be searched

I. Vandalism: This classification includes all forms of intentional damage to property of vehicles except arson (refer to "C").

1. Vandalism to County property (594 P.C.)
2. Vandalism to private property (594 P.C.)
3. County vehicle
4. Private vehicle

J. Miscellaneous: Crimes/activities not covered in any of the above classifications.

1. Suspicious activity by a non-employee
2. Suspicious activity by a County employee (explain)
3. Hostage situation
4. Bomb threat
5. Suspicious package
6. Bomb or explosive device actually found
7. Power failure
8. Equipment failure
9. Other activity not covered in any other classification (explain)

K. Person sick or injured not the result of criminal activity.

1. Rescue responded
2. Sent to hospital
3. First aid given by other than rescue
4. Handled by security
5. Refused treatment
6. Other

L. Confiscation of contraband:

1. Weapon (gun, knife, club, etc.)
2. Narcotics (any non-prescription drug)
3. Other

X. FOR USE BY COURTS ONLY:

1. Restraints used
2. Escape
3. Attempted escape
4. Physical altercation within a Court facility
5. High risk trial
6. Threats (verbal or written) to a judge
7. Threats (verbal or written) to a juror
8. Attempted unlawful entry



County of Los Angeles
CHIEF ADMINISTRATIVE OFFICE

713 KENNETH HAHN HALL OF ADMINISTRATION • LOS ANGELES, CALIFORNIA 90012
(213) 974-1101
<http://cao.co.la.ca.us>

DAVID E. JANSSEN
Chief Administrative Officer

Board of Supervisors

GLORIA MOLINA
First District

YVONNE B. BURKE
Second District

ZEV YAROSLAVSKY
Third District

DON KNABE
Fourth District

MICHAEL D. ANTONOVICH
Fifth District

July 1, 2004

Mr. Richard Shinee, Attorneys at Law
A Professional Corporation
16055 Ventura Blvd, Suite 1000
Encino, California 91436-2680

Dear Mr. Shinee:

**JUNE 29, 2004, BOARD AGENDA ITEM NO. 18
(CHIEF INFORMATION OFFICER
INFORMATION TECHNOLOGY SECURITY POLICY)**

Agenda Item No. 18 (Information Technology Security Policy) has been continued to Tuesday, July 13, 2004, for further consideration by the Board of Supervisors.

In response to your June 28, 2004, letter we have contacted Mr. Paul Roller, Chairman of the Coalition of County Union's, to determine which County Departments the CCU believes did not have Information Technology Security Policies in place. The information Mr. Roller provided included the Fire and Mental Health as departments which did not have such policies in effect, although Mr. Roller indicated that there could be other departments.

We have contacted the Fire Department and confirmed that they have an established Internet Security and Computer Use Policy. I have attached a copy of these policies for your information. We are also in the process of contacting the Department of Mental Health to determine if they have such policies in effect.

We have requested the Chief Information Officer and our employee relations staff to review the issues that you raised in your correspondence. As to those departments that already have established Information Technology Security Policies in place CAO/Employee Relations will support the CIO's request for Board approval of these minimum standard policies on July 13, 2004.

Mr. Richard Shinee, Attorneys at Law
July 1, 2004
Page 2

I have also asked Mr. Roller to include CAO/ER on the CCU's July Agenda to discuss labor-management process and substantive issues involving departments which may not have established Information Internet Security Policies in effect.

Attached also is a copy of the CAO/Employee Relations Division June 9, 2004, letter regarding its labor-management win-win approach for the discussion of draft policies and initiatives. It would be the CAO/ER Division's intent to follow the approach outlined in this letter.

If you would like to discuss this matter further, please contact me at (213) 974-2497. We will contact Mr. Roller as soon as we receive additional information regarding this issue.

Sincerely,

DAVID E. JANSSEN
Chief Administrative Officer

A handwritten signature in cursive script that reads "Donald L. Washington".

Donald L. Washington, Assistant Division Chief
Employee Relations Division

c: Paul Roller, Chair, Coalition of County Unions
Jon Fullinwider, Chief Information Officer

Attachment

Shinee Response Letter

September 28, 2000

EP - 545

**TO: ALL CHIEF OFFICERS
ALL ADMINISTRATIVE SITES**

FROM: CHIEF DEPUTY LARRY C. MILLER

**SUBJECT: UNAUTHORIZED SOFTWARE AND INTERNET (WEB) ACCESS
USING COUNTY EQUIPMENT AND COMMUNICATION LINES**

DISPOSITION: RETAIN IN BRIEFING MANUAL UNTIL FURTHER NOTICE

This directive is to reinforce existing policy regarding appropriate use of County equipment, including personal computers and telecommunication lines. This briefing also advises all personnel that the use of America On Line (AOL) Internet access software is specifically prohibited on Departmental computers.

General Operations Manual, Volume 2, Chapter 5, Subject 10, Computer System Security, specifically states that the Information Management Division (IMD) must approve all software and devices installed on Departmental computers. It also states that County computer systems (including data lines) are only to be used for County business.

A reminder of this policy is necessary due to the recent discovery that some sites have installed America On Line (AOL) software to gain unauthorized access to the Internet (Web) via County computers. Some sites are also using the Department's telecommunication lines to obtain unauthorized Web access. If a site has a business-related need to access the Internet, written authorization is required at the Bureau Chief level. The first step in the authorization process is to route a request through the appropriate division manager to IMD (email Crodrigu). Upon receipt, IMD will issue a packet of instructions to the requestor.

The Department's standard Internet access software is Internet Explorer or Netscape Navigator/Communicator. AOL is not an option as it is specifically designed to permanently override a computer's existing communication settings, which then corrupts the settings for our network environment. Once this happens, the problem cannot be corrected without completely re-imaging the computer's hard drive.

All Chief Officers

el mie Bruner - EA61

Page 1

January 27, 1999

EA - 61

TO: ALL CHIEF OFFICERS
ALL ADMINISTRATIVE SITES

FROM: CHIEF DEPUTY LARRY C. MILLER

SUBJECT: COUNTYWIDE POLICY REGARDING UNAUTHORIZED USE
OF TELECOMMUNICATIONS EQUIPMENT AND SERVICES

DISPOSITION: RETAIN IN BRIEFING MANUAL UNTIL JUNE 30, 1999:
THEN DISCARD

The purpose of this communicate is to restate the County's longstanding policy that telephones and other telecommunications equipment and services are for County business. Unauthorized use of phones and telecommunications equipment is strictly prohibited. Violation of this policy may subject employees to disciplinary action, including discharge. All supervisors/managers shall be aware of employee telephone usage, and shall counsel/discipline employees as warranted for unauthorized use of County telecommunications equipment and services.

The Auditor-Controller recently conducted an audit of County Departments and determined that there is considerable abuse of telecommunications equipment and services by County employees. Therefore, all employees are advised to review Volume 2, Chapter 5, Subject 18 of the Department's Manual of Operations regarding telephone use/abuse.

Questions regarding the County and Department policy regarding telephone use should be directed to Eric J. Hawkins, Compliance Officer, at (323) 881-2377. Questions concerning disciplinary action for violation of telephone policy should be directed to John Cherep, Employee Relations, at (323) 881-2470.

LCM:rl

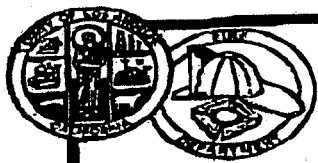
c: Miller

ALL PERSONNEL SHALL READ AND INITIAL

"A"

"B"

"C"



Computer Operations

Volume H

General Operations

Chapter 1

Microcomputer, General Operations

Subject 1

07/01/91

I. INTRODUCTION

- A. **Purpose:** To define and establish guidelines and procedures for the use of microcomputers in the Department.

Telephone Numbers: Telephone numbers for the various IMD offices can be found in Manual A.

- B. **Scope:** This instruction applies to all employees of the Department.

- C. **Author:** The Administrative Deputy, Administrative Bureau, through the Chief, Information Management Division, is responsible for the content, revision, and annual review of this instruction.

II. RESPONSIBILITY

- A. **All personnel** are responsible for the policies contained herein.

- B. **Administrative Site supervisor(s)** are responsible for the enforcement of the policies contained herein.

III. POLICY

- A. **General Policies.**

1. **System Standards.** The Department's standard microcomputer workstation is a DOS compatible system with printer, optional modem, a minimum 40 megabyte (MB) hard disk drive, and one 3 1/2" diskette drive (an additional 5 1/4" diskette drive is optional) (See Appendix I - Hardware Standards)
2. **Software Standards.** The Information Management Division maintains a list of software packages which have been adopted as Departmental "standards". Wherever possible, all applications should be developed using these standards. IMD may add additional software to this list at any time, depending on the needs of the Department. On an individual basis, IMD may approve the use of an alternative software package to meet unique circumstances within the Department.

Page 1

Received Jun-29-2004 04:28pm

From-3238873704

To-LACOFD EMPLOYEE RELA Page 012

Received Jun-28-2004 04:26pm

From-3238873704

To-LACOFD EMPLOYEE RELA Page 013



07/01/91

Computer Operations

Volume H

General Operations

Chapter 1

Microcomputer, General Operations

Subject 1

APPENDIX I

DEPARTMENTAL HARDWARE STANDARDS

FIELD ADMINISTRATIVE SITES:

MICROCOMPUTER:

Precision 386SX Microcomputer, minimum 16 Mhz
 2 MB Installed RAM
 8 Expansion Slots
 NEATSX/INTEL Chipset or equivalent
 40 MB Hard Disk with average seek time less than 30 MS
 1.44 MB Floppy Disk Drive (3.5")
 1 Parallel and 1 Serial port
 101 Key Enhanced Keyboard
 200 Watt Power Supply
 2400 Baud internal modem, certified 100% Hayes Compatible and AT Set Compatible
 MS DOS 4.0 or later
 Mitsubishi 14" VGA Monitor (Model #1429C or equivalent)
 BOCA VGA 16 Bit Video Adapter (800 X 600 or equivalent)
 1:1 Interleave Disk Controller, Minimum Seek Time < 30MS

PRINTERS:

Panasonic KX P1124, KX P1624



07/01/91

Computer Operations

Volume H

General Operations

Chapter 1

Microcomputer, General Operations

Subject 1

APPENDIX II

DEPARTMENTAL SOFTWARE STANDARDS

FIELD ADMINISTRATIVE SITES(*):

Professional Write
Direct Access

(*) These two packages are the only packages currently approved for use by Field Administrative Sites. However, IMD may utilize other software packages for departmental applications residing on the "C" drive of Field Administrative Sites.

NOTE: Software on the "C" drive is limited to Departmental applications.

ADMINISTRATIVE (NON-FIELD) SITES:

WORD PROCESSING:
Professional Write
Word Perfect

DATA BASE:
Paradox
PFS File

GRAPHICS:
Harvard Graphics
Pagemaker

SPREADSHEET:
Quattro



Computer Operations

Volume H

General Operations

Chapter 1

Microcomputer, General Operations

Subject 1

07/01/91

APPENDIX III

ORDERING MICROCOMPUTER SUPPLIES

ITEMS AVAILABLE FROM THE STOCKROOM:

Printer Ribbons
Printer (Laser) Cartridges
Data Diskettes

ITEMS AVAILABLE FROM THE WAREHOUSE:

Computer Paper (Continuous Feed)

All other computer support products must be ordered via the Requisition Form (68) process.
For example:

Diskette Holders
Document Holders
Glare Screens
Diskette Cleaning Kits
Power Directors
Power Surge Strips
Monitor Cleaners
Paint Brushes (for dusting keyboards and back of CPU)

Page 9 End



07/01/91

Computer Operations

Volume H

General Operations

Chapter 1

Microcomputer Support and Training

Subject 3

I. INTRODUCTION

- A. Purpose: To define and establish the guidelines and procedures for the use of microcomputer support and training.

Telephone Numbers: Telephone numbers for the IMD offices may be found in Manual A.

- B. Scope: This instruction applies to all employees of the Department.

- C. Author: The Administrative Deputy, Administrative Bureau, through the Chief, Information Management Division, is responsible for the content, revision, and annual review of this instruction.

II. RESPONSIBILITY

- A. All personnel are responsible for the policies contained herein.

- B. Administrative Site supervisor(s) are responsible for the enforcement of the policies contained herein.

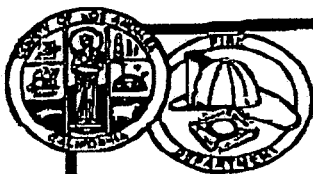
III. POLICY

Responsibility for support of microcomputers has been established in the Information Management Division (IMD) of the Administrative Bureau. Support includes consulting, training, problem resolution, procurement assistance, and review of user justification and operation of the computing resource. The IMD will assist in the justification and evaluation process; however, ultimate justification and the proper operation and management of the microcomputer will be the user's responsibility. Details of these responsibilities and services are outlined below.

- A. Information Management Division Responsibilities.

1. In general, IMD maintains sole responsibility for the following:

- a. Ensuring an efficient and effective (automation) operating environment, compatible with the Department's mission and goals.



07/01/91

Computer Operations

Volume H

General Operations

Chapter 1

Microcomputer Support and Training

Subject 3

- c. Developing technical specialists within each Section, who can then provide guidance and assistance to their respective staff;
- d. Conducting periodic reviews of user operations on behalf of the Fire Chief, to ensure that the automated systems are being properly operated and managed and that the policies and guidelines set forth in this instruction are being followed;
- e. Assisting with the acquisition of system components and assisting in the installation of the equipment and software;
- f. Coordinating the relocation of hardware and software;
- g. Establishing and advising users on policies related to security, documentation and backup procedures; and
- h. Coordination and delivery of maintenance and repair of all computer related products.

B. User Responsibilities. The user shall be responsible for the following:

- 1. Implementation of policies and standards as defined in this instruction;
- 2. Utilizing available training resources and reference materials to resolve day to day operational issues related to proper use of software/hardware;
- 3. Documenting automation problems as they occur, including what procedure and software package were in use when the problem occurred;
- 4. Maintaining adequate work supplies;
- 5. Ensuring that the hardware is properly maintained, including periodic cleaning (as outlined in Appendix I).



Computer Operations

Volume H

General Operations

Chapter 1

Microcomputer Support and Training

Subject 3

07/01/91

APPENDIX I

RECOMMENDED MICROCOMPUTER USER MAINTENANCE

MONITORS:

Screen:

Should be cleaned with a non-abrasive cleaner and cloth at least once a week.

ALWAYS spray the cleaner on the cloth then wipe the screen.

DO NOT spray the cleaner directly on the screen.

NEVER clean the screen with alcohol.

Exterior Casing:

Attracts dirt and should be wiped off with a damp (not wet) cloth at least once a month

KEYBOARDS:

You should never eat or drink over the keyboard, as the food particles will jam the keys, and fluids will "fry" it!



07/01/91

Computer Operations

Volume H

Chapter 1

General Operations

Subject 3

Microcomputer Support and Training

APPENDIX II

| | | | |
|----------------------------------|--|---------------|-------------|
| | COUNTY OF LOS ANGELES FIRE DEPARTMENT INFORMATION MANAGEMENT DIVISION REQUEST FOR ESTIMATES | | NO. 1 |
| | TYPE OF REQUEST: <input type="checkbox"/> NEW <input type="checkbox"/> REVISION <input type="checkbox"/> MISC. | | DATE: _____ |
| REQUESTOR _____ | | SECTION _____ | PHONE _____ |
| DESCRIPTION OF REQUEST (attach): | | | |

AREA (Program/Module/Component) :

EXPECTED RESULTS (Example: Additional Sheets if Necessary) :

| | | | |
|-----------------------------------|---------------------|---------------------|----------|
| Work Group/MD | | | |
| PRIORITY _____ | DATE REQUIRED _____ | DATE APPROVED _____ | BY _____ |
| VENDOR _____ | | DELIVERY DATE _____ | |
| THE COST _____ | | | |
| DIRECT OR OTHER MODULE COMPONENTS | | | |

| | | |
|----------------|----------------|------------|
| APPROVED _____ | RECEIVED _____ | DATE _____ |
|----------------|----------------|------------|

Form 670 5/91

Page 7 End



Computer Operations

Volume H

GENERAL OPERATIONS

Chapter 1

07/01/91

Subject 0

TABLE OF CONTENTS

SUBJECT NUMBERTITLE

1

MICROCOMPUTER,
GENERAL OPERATIONS

2

MICROCOMPUTER SECURITY

3

MICROCOMPUTER SUPPORT AND
TRAINING

Page 1 End



07/01/91

Computer Operations

Volume H

System Procedures

Chapter 2

Electronic Mail (Fire Mail)

Subject 1

I. INTRODUCTION

- A. Purpose: To provide guidelines and operational instructions for the Fire Mail system.

Background: The Fire Mail system is an electronic mail (E-Mail) service to which the Department subscribes through Western Union. The Fire Mail system is the current replacement for the outdated teletype system. Highland Mail is the software program which provides the shell for this system.

- B. Scope: This instruction applies to all employees of the Department with access to the Fire Mail system.
- C. Author: The Administrative Deputy, Administrative Bureau, through the Chief, Information Management Division, is responsible for the content, revision, and annual review of this instruction.

II. RESPONSIBILITY

- A. All personnel are responsible for the policies contained herein.
- B. Administrative Site supervisor(s) are responsible for the enforcement of the policies contained herein.

III. POLICY

- A. Authorized locations. Fire Mail is authorized for use at the following locations:
1. Battalion Headquarters.
 2. Division Headquarters.
 3. Fire Suppression Camps.
 4. Fire Prevention Headquarters and Area Units.

Jul-01-2004 03:04pm

From-LACOFD EMPLOYEE RELATIONS DIVISION

323 415 8552

T-601 P.014/034 F-198

Received Jun-28-2004 04:26pm

From-3238873704

To-LACOFD EMPLOYEE RELA Page 023

I. INTRODUCTION

- A. Purpose: To insure appropriate security of computer equipment.
- B. Scope: This instruction applies to all personnel, both uniformed and civilian, at all administrative sites.
- C. Author: The Deputy Director of the Administrative Bureau, through the chief of the Information Management Division (IMD), shall be responsible for the content, revision, and annual review of this instruction.
- D. Definitions:

HARDWARE: The physical components of computers and related devices.

SOFTWARE: The general term for the various kinds of programs used to operate computers and related devices. Anything that can be stored electronically is software.

LICENSING AGREEMENTS: Contractual restrictions imposed upon software by the owner of the copyright.

II. RESPONSIBILITY

- A. All Personnel shall protect the computer system from damage, theft or unauthorized use.
- B. Site Managers/Supervisors shall take all appropriate measures to protect this system from: theft of physical equipment, unauthorized use of access to Department information and unauthorized use of County equipment, services or information.

III. POLICY

- A. Unauthorized Access/Use: County computer systems are to be used by County employees doing County business. Department information is not to be released to non-department personnel without permission of the Fire Chief or his designee. Site supervisors are to provide adequate security measures to prevent unauthorized use of this system.

(11/01/98)

1

V2-C5-S19

B. Physical Security

1. Rooms housing the computer equipment are to be completely secured at any time the station or site is not occupied or directly observable via visual or electronic means.
2. Cabinets or other storage areas will be provided for consumable or removable items such as recording media, printer paper, and operations manuals. All material is to be secured when not in use.
3. Locking brackets, cables, or other hardware shall secure portable equipment such as the computer, printer, and other related devices to prevent unauthorized removal.

B. Security of Software

1. All software that is loaded on computers at all administrative sites shall be approved by IMD. Unapproved software or devices shall not be loaded on/or used by County computers as damage to the operating system and other Department software may occur.
2. Copyrighted software shall not be duplicated as it is against the law. Site supervisors are responsible for protecting the County from legal action by prohibiting unauthorized duplication of such material. Questions regarding compliance with this section are to be directed to the Information Management Division (IMD).
3. Licensing agreements pertaining to commercial software use shall be adhered to (see individual packages for specific restrictions).
4. Storage media (diskettes, tapes, etc.) shall be removed from the computer and secured when not in use.
5. All essential data files, whether stored on diskette or hard drive shall be duplicated on floppy disk and stored separately to prevent loss of data.
6. Data files often contain sensitive Department or personal information. This information is to be protected. Unauthorized entrance into Department files or systems is prohibited.
7. All users are encouraged to develop on-site data management practices, which limit access to sensitive information.

(11/01/98)

2

V2-C5-S10

8. Recorded material that is outdated shall be purged by erasure/degaussing. Outdated material in printed form shall be physically destroyed before disposal.
9. Where passwords are required or utilized, each user is responsible for password security. Passwords shall not be shared. Passwords are to be changed on a regular basis and whenever personnel changes occur.
10. Computer system components may not be removed from assigned sites without prior permission from the Fire Chief or his designee.
11. Data transmission between sites requires prior authorization from the responsible agents.
12. County information may not be processed, transmitted or stored by, to, or in privately owned computer systems without prior written authorization by the Fire Chief.

IV. PROCEDURES

- A. Specific procedures for the operation of the computer system accompany the equipment and are to be kept at the location where the system is housed.
- B. The following components are construed as being part of the Computer Communications System and are subject to the controls and policies of this section. Specific definitions are located in the manuals and instructions that accompany the equipment.
 1. Computer, Keyboard, Monitor
 2. Surge Power Director
 3. Internal peripheral components (modem, zip drive, etc.)
 4. External components (speakers, CD-ROM, etc.)
 5. Printer
 6. All data generated by, or obtained through the system
 7. Computer Phone Lines

(11/01/98)

3

V2-C5-S10

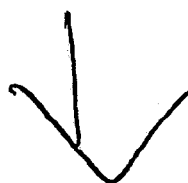
8. Recording media/devices
9. Software
10. Printed Material
11. Contracted Services

(11/01/98)

4

V2-C5-S10

internet Pkg





COUNTY OF LOS ANGELES
Internal Services Department
Information Technology Service

**EMPLOYEE ACKNOWLEDGEMENT OF
ISD INTERNET ACCEPTABLE USAGE POLICY (AUP)
SECURITY RESPONSIBILITIES**

It is the policy of the County of Los Angeles (County) that each employee, whether permanent, temporary, part-time, contract or any other, be individually responsible for the protection of all County information, data, and information processing resources to which he or she has access by virtue of employment by the County.

I hereby acknowledge that I will be held accountable for my actions when using the Internet through ISD resources. I hereby state that I will use due diligence to conform my actions to the following usage rules governing ISD Internet access:

- Only I will use my ISD Internet ID. I will not share my Internet ID and/or password with any other person.
- I will not transmit or make available sensitive County data over the Internet.
- I will not transmit data and/or communication violating any applicable law or regulation (including copyright laws).
- I will not communicate or transmit any text, graphic, audio, video, or other data which may be deemed in any reasonable way offensive, unless it is in the performance of my job duties, e.g., law enforcement.
- I will not leave my Internet session unattended.
- I will not jeopardize network services by knowingly or carelessly distributing computer worms or viruses.
- I will use ISD Internet access for County management-approved purposes only.
- I will scan all downloaded files for viruses.
- I will follow all Internet netiquette rules listed in the *Acceptable Usage Policy for ISD Internet Service*.
- I will follow the *Countywide Data Security Policy* (dated February 25, 1991).
- I will follow all guidelines in the *Acceptable Usage Policy for ISD Internet Service* not specifically listed above.

I understand that my Internet activities, including e-mail, may be logged, are a public record, and are subject to audit and review by authorized individuals.

I recognize that my willful or negligent failure to fulfill these responsibilities, including the actions of someone else using my ID, could result in the abuse of County Information resources and data, and that the County may hold me personally responsible for such abuse.

Employee Name (PRINT)

Employee Signature

Date

Manager's Name (PRINT)

Manager's Signature

Date

aupform / 04-04-00

FREQUENTLY ASKED QUESTIONS OF ISD INTERNET SERVICE (FAQ)

How soon will I get my ID? What is my password? How do I know when they will be ready?

- If all the necessary information is provided in both the *Internet Registration Form* and *AUP Form*, Christine Rodriguez and ISD Data Security will process your paperwork within 2 weeks of being submitted. Christine Rodriguez of IMD will email you to inform you of your username and password.

How much does ISD charge for connection to the Internet?

- ISD charges a flat monthly fee of \$5 per customer, to each County Department for access to the Internet (i.e., WWW, newsgroups, etc.). The user does not have to pay this fee. This single monthly fee provides you with 24-hour access to the Internet whether you are using direct or dial-up connection.

Can I use Netscape Navigator or Internet Explorer to navigate the Internet?

- The Department recommends that you use Internet Explorer to navigate the Internet.

Can I share my username and password with others?

- No, usernames and passwords are confidential and may not be shared with others. The Acceptable Usage Policy Agreement you are required to sign with your Registration specifically states that each account holder is not to share his/her internet ID with any other individual or group.

Will ISD set up an Internet Group ID account to be shared by my group?

- No, group accounts will not be issued. Each person interested in accessing the Internet must apply on his/her own. The CAO and Auditor-Controller mandate that no Internet Group IDs be issued "for security and accountability reasons." Regardless of whether you use ISD as your Internet Service Provider (ISP) or decide to use non-County ISP, you are still required to comply with this mandate.

Can my immediate supervisor or manager sign my registration forms?

- Department Policy requires Deputy level approval on both the *AUP Form* and *Internet Registration Form*.

Who can I call if I am having problems with my Password or accessing the Internet?

- If you are having problems or have forgotten your password, you must contact the ISD Helpdesk at 562-940-3443. The ISD helpdesk is available 24 hours per day, 7 days per week. Please note that the County-wide Data Security Policy dictates that another person cannot call for you. You alone must make the call.

C:\Internet\FAQ
12/3/2003

CHIEF ADMINISTRATIVE OFFICE
INFORMATION RESOURCES

February 25, 1991

DATA SECURITY POLICY

Page 1 of 3

PURPOSE

The intent of this policy on Data Security is to ensure that all managers and employees are aware of their role and specific responsibilities in protecting the County's information assets.

The policy on data security set forth herein applies to all data collected, used, maintained and accessed by computer systems of Los Angeles County. This policy is required so that the County meets its obligations to the public to maintain uninterrupted delivery of services while safeguarding sensitive information against potential misuse, abuse or loss.

POLICY

Managers of each County department shall ensure that County computer data in the department's custody is protected through application of fundamental principles of data security. Those principles are delineated in the standards section of this policy.

Responsibility for authorizing release of data under the Public Records Act resides exclusively with the department owning the data. Any questions as to the propriety of such release shall be submitted to the County Counsel for review.

STANDARDS

Individual Accountability Each employee (permanent, temporary, part-time, contract or any other) is individually responsible for the protection of all County information, data, and information processing resources to which he or she has access by virtue of employment by the County. Users of data will protect County computer data as required by the data owner.

Need to Know/Use Data owners shall determine the degree of protection required for their data and determine who may have custody or access to data, which they own. Access to County computer data and associated processing privileges shall be granted only as required to perform the tasks and responsibilities currently assigned to an individual, or to an operating unit. Individuals with custodial access to data owned by another department shall protect the data as required by the data owner.

Data Classification and Protection Managers of each department shall define and prepare in written form, the protection requirements for data that they own in each of three categories: confidentiality, integrity and availability. Each department having custody of or using County computer data shall implement and maintain data security measures commensurate with the protection requirements of the data owner. Department managers are required to inform other departments of the protection requirements for their data.

CHIEF ADMINISTRATIVE OFFICE
INFORMATION RESOURCES

DATA SECURITY POLICY

February 25, 1991

Page 2 of 3

Adequacy of Controls Managers of each department shall ensure that their departments meet the protection requirements for all County computer data in their custody. The controls, internal and external, must be shown to be complete, uniform and constantly applied. They must prevent an accumulation of responsibility and functions by any one individual, which could facilitate the undetected commission of malicious, negligent or fraudulent acts.

Security Awareness Managers of each department shall ensure employee awareness of the importance of County computer data security. All employees designated by the department based on the employee's access to County computer data shall sign an acknowledgement that they have read and understand their responsibilities under this policy, and other security policies and standards the department has implemented.

Risk Analysis Management of County departments shall periodically conduct a risk analysis of their computer systems. The purpose of the risk analysis is to identify the protection requirements for County computer data owned by their departments and to evaluate the technical and procedural internal and external controls in place to provide protection of owned and custodial data. The frequency of such analysis shall be determined by the department based on the security classification of the system and operational considerations. Such determination shall be documented and kept on file with the departmental systems manager.

COMPLIANCE

The Auditor/Controller periodically audits County departments' compliance with security policies. Particular emphasis shall be placed on the effectiveness and completeness of the classification and protection of County computer data.

NOTES

Definitions applicable to this Policy:

1. **Availability of data.** The availability for its intended use, when and where needed.
2. **Classification of data.** The process of defining the relative importance of protection required for specific data. The consequences of failing to protect it are assessed on a scale ranging from no impact to catastrophic impact.
3. **Computer system.** This term shall be broadly interpreted to include all generalized data processing and office automation systems. Systems on portable computers through the largest mainframe computers are included.

CHIEF ADMINISTRATIVE OFFICE
INFORMATION RESOURCES

February 25, 1991

DATA SECURITY POLICY

Page 3 of 3

4. Confidentiality of data. The sensitivity of information to harm, which may result from its unauthorized disclosure.
5. County computer data. All data entered and maintained in any County computer system, and all programs and documentation constituting those systems, whether developed by or for the County or licensed to the County. Data may be in any form, in storage media, in computer memory, in transit or presented on a display device.
6. Custodian of data. A department is in custody of data when it has possession of a copy of the data in any form from which it can be perceived, reproduced, or otherwise communicated.
7. Data owner. For purposes of this policy, the ownership of County computer data is delegated to County department heads. In general, the data contained within a computer system is owned and managed by the department for whom the system was developed. Ownership of data stored in a computer system shared by several departments is retained by the department originating the data. Custody of data is vested in the department in which the shared computer system is physically located.
8. Data security. The protection and preservation of confidentiality, integrity and availability of County computer data.
9. Data user. An individual or organizational unit who is granted access to data to carry out assigned duties and responsibilities.
10. Integrity of data. The accuracy (no errors or unauthorized changes), completeness (nothing added or deleted), and currency (all known changes are present) of records.

CHANGING YOUR INTERNET PASSWORD

It is responsibility of each user to preserve the confidentiality of his/her password. If you feel your account is being inappropriately accessed, it is your responsibility to change your password immediately. Therefore, if you suspect that your password has been lost, etc, you should immediately take action to change it.

It is also recommended that you periodically change your Internet password for added security.

The following instructions will assist you in changing your password via the LA County Intranet website:

- First go to the LA County Intranet website. The address for this site is <http://web.co.la.ca.us/lacounty/>
- Once you are at this site click on "Change Firewall Password".
- Now click on "Change Password - Direct Connection"
- A new window will open and this is where you will change your password. Follow the instructions as provided on this page. Upon completion of the steps as directed, your password will be reset immediately.

If you experience any problems with changing your password via the County's Intranet site, you can call the ISD Helpdesk for further assistance at (562) 940-3443 and request that your Internet Firewall password be re-set.

Last updated on:
December 3, 2003

ACCEPTABLE USAGE POLICY FOR ISD INTERNET SERVICE (AUP)

PURPOSE

The purpose of this policy is to establish standards for the acceptable usage of the Internet by employees of the County of Los Angeles (County) when such usage is made through access provided by the Internal Services Department (ISD) and while using County funds and/or on County time.

REFERENCES

Countywide Data Security Policy

County of Los Angeles Public Library; "Appropriate Staff Use of the Internet"

Intel Corporation. "Intel's Internet Guidelines", Revised 7/11/84

Mindspring's Appropriate Use Policy

Rinaldi, Arlene. "The Net User Guidelines and Netiquette", Florida Atlantic University, July 1994

Sequel Corporate Policy Guideline, Internet & E-Mail Acceptable Use Policy

POLICY

This policy is applicable to all permanent and temporary County and Contractor employees accessing the Internet through ISD-provided services. Any reference to "County employee" in this document is intended to also include any employee of a Contractor performing work for the County.

In addition to the guidelines set forth in the Countywide Data Security Policy, dated February 25, 1991, County employees will adhere to this policy of acceptable usage when accessing the Internet through ISD. Adherence to this policy ensures the following objectives:

- Respecting County computing resources
- Maintaining the integrity of the County of Los Angeles
- Ensuring the security of County internal computer systems
- Minimizing the risk of legal action taken against the County or any employee

DEFINITIONS

Definitions applicable to this policy are:

1. **Accountholder:** The County employee or Contractor employee granted access to the Internet, the County's Intranet, ISD's Internet e-mail, or any Internet services such as newsgroups, through services provided by ISD.
2. **E-mail (electronic mail):** Electronically stored messages, which can be passed from one computer to another. E-mail may include non-interactive communication of text, data,

images or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "mail," facsimile," or "messaging" system; or voice messages transmitted and stored for later retrieval from a computer system.

3. **ftp (file transfer protocol):** The Internet's mechanism for moving a file from one place on the Internet to another. e.g., from a remote computer to your computer.
4. **Internet:** A worldwide network of networks, connecting informational networks communicating through a common communications language, or "protocol."
5. **Intranet:** A network of networks that is contained within an enterprise, i.e., within the County and is inaccessible to those outside the enterprise. The main purpose of an Intranet is to share and disseminate information throughout the enterprise.
6. **Mailing list:** A list of individuals who subscribe to a distribution service focusing on a particular topic or interest.
7. **Netiquette:** Network etiquette conventions used in written communications.
8. **Newsgroups:** Discussion groups, which are posted on Usenet. There are currently over 25,000 such groups covering nearly every topic imaginable.
9. **Telnet:** A terminal emulation program, which resides on your computer. It allows you to connect to a remote computer over the Internet. You can then enter commands through the Telnet program and they will be executed as if you were entering those commands directly on the remote computer itself. To begin a Telnet session, you must log in to the remote computer by entering a valid user name and password.
10. **Usenet:** A worldwide network of discussion groups, called newsgroups, containing millions of posted messages.

PROCEDURES

Internet, Intranet, and e-mail access provided by ISD is intended to be used for business purposes only. ISD encourages the use of the Internet, Intranet, and e-mail because they make communication more efficient and effective. However, these services are County property, and their purpose is to facilitate County business. Every account holder has a responsibility to maintain and enhance the County's public image and to use e-mail and access to the Internet and Intranet in a productive, professional manner. To ensure that all account holders act in a responsible manner, the following guidelines have been established for using the Internet, Intranet, and e-mail. Any improper use of these services is unacceptable and will not be permitted.

- Account holders must take all basic precautions for ensuring responsible use of the Internet. Such responsible use includes, but is not limited to, the following:

Refusing to share your Internet ID and/or password with anyone.

Using complex passwords rather than obvious passwords. For example, it is poor practice to use a password someone can easily determine such as your child's or pet's name. A good password consists of several characters and numbers mixed together, taking advantage of special characters and case-sensitivity. For example: "sk3m8T".

Avoiding writing your password down and storing it in an insecure location. If you must write down your password to avoid forgetting it, do not leave it in an insecure location.

Changing your password frequently.

Logging off an Internet session whenever you leave your computer unattended.
Log off your Internet session and exit your Internet software as soon as you are done using it.

- In communicating with others via the Internet, accountholders should remember they are representing the County and they must conduct themselves in a responsible, polite, and ethical manner, abiding by all local, state, and federal laws. This is especially apparent with e-mail since each accountholder's e-mail address bears the "@co.la.ca.us" suffix.
- Accountholders must use copyrighted material in accordance with copyright laws and abide by the provisions of any applicable license agreements.
- Accountholders should view the Internet services provided by ISD as a County resource, not unlimited in nature, ensuring efficient and respectful use of time on the Internet.

For Direct Connection accountholders, your LAN is connected to LAInternet via the same connection that you and others on your LAN use to access County systems, such as those on the IBM mainframe. Check with your LAN Administrator to determine how your Internet access (time of day, length of connections, number of bytes transmitted) may impact others' access of LAInternet.

For Dial-up Connection accountholders, you should remember that there are a limited number of modems at ISD to receive your call. Because others may be waiting for a modem connection to become available, disconnect when you are through using the ISD Internet service.

- The County does not have control of the information on the Internet. Non-County sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or offensive to some people. It is the accountholder's responsibility to use good judgment in accessing appropriate information relevant to conducting County business.
- Accountholder IDs are to be used only by the authorized owner of the ID. No IDs are to be shared. Accountholders are ultimately responsible for all activity occurring under their ID.
- Accountholders must maintain their e-mail accounts in a responsible manner. Guidelines for responsible e-mail account maintenance are as follows:

Accountholders are expected to regularly log on and retrieve their mail. Failing to do so may result in disk space allocated for your e-mail becoming overloaded. This may prevent you from accessing your e-mail and may result in the permanent loss of your e-mail.

Since each accountholder's e-mail is accessible by any person with system privileges, accountholders are reminded to keep this in mind when sending, receiving, or storing e-mail or any information on the Internet/Intranet servers. Accountholder mail is not deemed to be private or confidential and may be viewed by an accountholder's manager upon a showing of reasonable suspicion.

that the accountholder has violated one or more of ISD's Internet Acceptable Usage policies.

VIOLATIONS OF ISD POLICIES

The following are violations of ISD's Internet Acceptable Usage Policy:

1. Revealing an accountholder's password to others or allowing use of the accountholder's password by others.
2. Using ISD's Internet services for illegal purposes, or in support of illegal activities. Such activities include, but are not limited to:
 - The unauthorized copying of copyrighted materials including, but not limited to, any photographs or graphics from on-line magazines, newspapers, books, or other copyrighted sources.
 - The exporting of any software or technical information in violation of U.S. export control laws.
 - The posting of scams such as pyramid schemes or "make-money-fast" schemes or e-mailing of such scams to others via the Internet.
 - The posting or transmitting of any message or material which is libelous, defamatory, or which discloses private or personal matters concerning any person.
 - The posting or transmitting of any message, data, image, or program, which is indecent, obscene, or pornographic.
3. Posting or e-mailing charity requests, petitions for signatures, chain letters, advertising, promotional materials, or any other solicitation of other Internet users except where approved and authorized County business is involved.
4. Using ISD Internet services for financial, commercial, political, or general personal gain.
5. Threatening bodily harm or property damage to individuals or groups. Posting or e-mailing any material or remark deemed offensive in any way, including those containing:
 - Derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference
 - Sexual content
 - Abusive, profane, obscene, or offensive languageunless such material or remarks are necessary for legitimate County purposes, e.g., when used for legal or law enforcement purposes.
6. Posting or e-mailing any material which would be deemed to reflect negatively on the County.
7. Posting or transmitting any material deemed to be sensitive, proprietary, or confidential County information.

8. Posting or transmitting any message anonymously or under a false name.
9. Attempting an unauthorized access to the account of another individual or group on the Internet, or attempting to penetrate beyond ISD security measures or security measures taken by others connected to the Internet, regardless of whether or not such intrusion results in corruption or loss of data.
10. Knowingly or carelessly distributing viruses to or from ISD servers.
11. Harassing others by 'mail-bombing' or 'news-bombing'. 'Mail-bombing' constitutes sending more than ten similar e-mail messages to the same e-mail address. 'News-bombing' constitutes sending more than 10MB of data to a newsgroup.
12. Forging any e-mail or newsgroup header.
13. Posting articles to any newsgroup, mailing list, or similar forum, which are off-topic according to the charter or other public statement of the forum.

Acceptable Behavior Guidelines for Specific Internet Functions

E-mail (Electronic mail):

The following guidelines apply to sending electronic mail (e-mail) via the Internet:

- Assume all mail sent or received by you is not secure. Do not include anything in an e-mail message, which you want to keep private or confidential. Unless you encrypt your e-mail, your mail is susceptible to being read by others.
- Use consideration when sending replies. Make sure you're sending to a group when you want to send to a group and to an individual when you want to send to an individual. If in doubt, address the recipient directly rather than use the "reply" command.
- To help better identify yourself, use signature blocks at the bottom of your e-mail messages. A signature block should include pertinent information such as the account holder's name, department, postal address, phone/fax number, and e-mail address.
- Be careful when using capital letters—THEY MAKE IT APPEAR YOU ARE SHOUTING. When emphasizing, use capitals sparingly. Other recommended punctuation for emphasis: "Asterisks" or underscore characters (e.g., "today", today).

Internet Mailing Lists and Usenet News Groups:

All the guidelines listed above covering e-mail should apply here as well. In addition:

- Consider how much business time could be required for reviewing particular lists or newsgroups, and how much mail a particular mailing list might generate. (It is important to log on frequently to retrieve your e-mail from mailing lists. You have limited disk space on the ISD mail server.) For good information on how to get started using newsgroups, look at the news.announce.newusers group.
- Read the Frequently Asked Questions (FAQs) for your newsgroup(s) before posting. Many of your questions may be answered there.

- Save the welcome messages/information files received when first subscribing to a newsgroup or mailing list. This information will often contain contact, unsubscribe, and other valuable information.
- Before posting to a group, observe the conventions of that particular group.
- Be clear and concise. Read all messages carefully before responding and review your reply before sending it to avoid any misunderstanding.
- Because your recipient cannot see you, be careful when using sarcasm and humor. Identify intended humor with standard statements (e.g., "only kidding folks") or with the universal smiley face: :-) [look sideways]
- To avoid any legal issues:
 - Cite all quotations, references, and sources. Also, when quoting from a previous message, include only the relevant portions, clearly identifying the quoted portions.
 - Obtain the original author's permission before forwarding the author's personal e-mail messages to discussion groups.

Telnet:

When using Telnet to access remote computer systems, users should remember that they are guests on another institution's machine. Telnet users should observe the following basic guidelines:

- Respect stated restrictions, as well as time and resource limitations of remote systems. Log off when finished. Staying logged on when you are not actively accessing the information may prevent others from connecting to that system.
- Read or obtain instructions or documentation files when using a system for the first time. Often the files will be listed when you first log on to the system. Often the file is named README.TXT, or a similar name. It is recommended that you file transfer the README.TXT file to your computer and disconnect the Telnet session. Read the downloaded file, and then reconnect to the remote computer. This frees logon resources.
- Because it may be interpreted as a break-in, do not use Telnet to access machines on which you do not have an account, or which do not support guest accounts. Also, do not attempt to use Telnet to access anonymous FTP servers; use FTP instead.

(FTP) File Transfer Protocol:

As with Telnet, FTP users are guests on other systems. FTP users should observe the following basic guidelines:

- After using FTP to transfer a file to a remote computer, and before downloading a file to your computer, make sure your computer is equipped with virus detection software. If possible, transfer files directly to a floppy diskette rather than to your hard drive. Then check the transferred files on the floppy disk for viruses.
- For FTP, logon as "anonymous" and respond to the PASSWORD prompt with your electronic mail address (e.g., jdoe@co.la.ca.us), unless the system specifies otherwise.
- Respect copyright and licensing agreements pertaining to transferred files.

- As with Telnet, respect stated restrictions, as well as time and resource limitations of remote systems.
- Observe working hours or posted hours for FTP sites.
- Avoid transferring files during peak business hours whenever possible.

RESULTS / IMPACT

ISD may monitor Internet, Intranet, and e-mail usage, including Web sites. Violation of this Acceptable Usage Policy could result in abuse of County computing resources, a serious breach of County network/computer systems security, or even a lawsuit against the account holder or County. Any account holder who abuses the privilege of ISD facilitated access to the Internet, Intranet, or e-mail may be subject to corrective action up to and including termination. ISD may hold an account holder responsible for such abuse. If necessary, ISD also reserves the right to advise appropriate legal officials of any illegal violations.

SUGGESTED READINGS

Kehoe, Brendan P. "A Beginner's Guide to the Internet: Zen and the Art of the Internet," Third Edition, 1995.

Krol, Ed. "The Whole Internet User's Guide and Catalog," O'Reilly & Associates, Inc., Second Edition, April 1994.

QUE Corp. "Using the Internet," Third Edition, 1996.

Smith, R., Gibbs, M., and Paul McFedries, P. "Navigating the Internet," Sam's Publishing, 1995.

CONTACT

Valerie Glass, Division Manager
Operations Support Division
Computing Services Branch
vglass@co.la.ca.us
562-840-3245



Information Technology Service

COUNTY OF LOS ANGELES / INTERNAL SERVICES DEPARTMENT
INTERNET REGISTRATION FORM
For L.A. County Employees

Type of Registration: ☐ New Registration ☐ Delete Registration ☐ Update Prior Registration

CUSTOMER INFORMATION

Last Name: _____ First Name: _____ MI: _____
Internet ID: _____ L.A. County Employee #: _____
(1st initial plus first 7 characters of last name; e.g. jdoe)
Department E-Mail Address: _____
Department Name: _____
Division Name: _____
Business Street Address: _____
City: _____ State: _____ Zip: _____ Phone #: _____
Customer Signature: _____ Date: _____

MANAGER'S APPROVAL

**WARNING: FAILURE TO FULLY COMPLETE AND SIGN THIS FORM WILL CAUSE A DELAY IN PROCESSING.
NO COPIES OR FAXES WILL BE ACCEPTED. ORIGINAL SIGNATURES ARE REQUIRED.**

Division Manager's Signature: _____ Date: _____
PRINT Manager's Name: _____
Manager's Title: _____ Phone: _____

PROCESSING

Submit completed forms to your Department's Internet Coordinator. Only ISD employees and Coordinators should submit this completed form directly to:
Data Security Registration Desk
ISD/Security and Business Recovery - MS 29
9150 E. Imperial Highway
Downey, CA 90242

Processed By: _____
Date: _____

**COUNTY OF LOS ANGELES / INTERNAL SERVICES DEPARTMENT
INTERNET REGISTRATION FORM INSTRUCTIONS
FOR L.A. COUNTY EMPLOYEES**

Type of Registration: New Registration • check if this is a new Internet registration
Delete Registration • check if you are deleting an Internet ID
Update Prior Registration • check if you are requesting a change to an existing Internet ID

CUSTOMER INFORMATION

Last Name, First Name, MI: Print or type your last name, first name, and middle initial.
Internet ID: Your Internet ID should be your CWTAPPS name. (Note: No Group IDs will be issued. However, an individual may request an alias name that is to be used by the individual only.)
Employee Number: Enter your six digit L.A. County employee number.
Department E-Mail Address: Enter your department's email address.
Department Name: Enter the full name of your County department, court, etc.
Division Name: Enter the full name of your County division.
Business Street Address: Enter your complete business street address, including room and/or suite number.
City, State, Zip, & Phone: Enter your city, state, zip code, and telephone number (including extension if applicable).
Customer Signature & Date: The customer requiring Internet access must sign and date this registration form before the form can be processed.

MANAGER'S APPROVAL

Failure to fully complete and sign this form will cause a delay in processing. Faxes will not be accepted. Original signatures are required.

Division Manager Signature & Date: The customer's Division manager or higher must sign and date this form.
Print Manager's Name: Print the name of the customer's Division manager or higher.
Manager's Title & Phone: Enter the manager's title and telephone number.

PROCESSING

This section is for ISD Data Security use only. Please send the original form to the address specified. No copies or faxes will be accepted.

11/03



County of Los Angeles
CHIEF ADMINISTRATIVE OFFICE

713 KENNETH HAHN HALL OF ADMINISTRATION • LOS ANGELES, CALIFORNIA 90012
(213) 974-1101
<http://cao.co.la.ca.us>

AVID E. JANSSEN
Chief Administrative Officer

June 9, 2004

Mr. Paul Roller, Chair
Coalition of County Unions
828 West Washington Boulevard
Los Angeles, CA 90015

Dear Mr. Roller:

**COUNTY MANAGEMENT DRAFT POLICIES
LABOR - MANAGEMENT APPROACH**

Before I propose the following for your consideration, I want to make it clear that under County Code (5.04.090), management sees a "material distinction" (UFC 6.125) between our obligation to "consult" and our obligation to "negotiate". Making this proposal in no way abrogates our rights and privilege under this ordinance. However, I am sure that we can agree our last few meetings have shown that efforts at defining management policies and initiatives as a "consult" vs. "negotiable" have not been meaningful. The current approach and subsequent discussions have not been productive for either party.

In order to strengthen and enhance labor-management relations with the CAO, Employee Relations Division and the Coalition of County Unions (CCU), we are proposing a "win-win" approach to the discussion of management drafted policies and initiatives.

County management is requesting that the CCU consider the following Labor/Management approach:

1. County management representatives will provide the CCU with copies of management drafted policies/initiatives for discussion.
2. CCU and County management will focus its attention on the details and requirements of the proposed draft policies and initiatives.

Appropriate areas of focus could include, but would not be limited to, the following:

- What is the policy/initiative impact on wages, hours or other terms and conditions of employment?
 - Are the terms and conditions of the policy/initiative new?
 - Are there ways to improve or change the policy/initiative to meet the interests of the parties?
 - Does it impact a substantial number of employees?
 - What is the purpose of the policy/initiative?
 - Have the substantive terms of the policy been previously negotiated or are they covered by Civil Service Rules?
 - Is the policy/initiative disciplinary or impose new conditions of discipline?
3. There would be no "waiver of rights" by either party from engaging in a substantive discussion over the terms of a management policy/initiative.
 4. If after a full and substantive discussion of the issues in the policy/initiative the parties arrive at a mutual resolution, implementation would occur in accordance with the parties understanding.
 5. If agreement is not reached, the CCU and the County could take whatever action it deemed appropriate as provided for under the County employee relations ordinance.

The benefit of this proposed approach would be to encourage labor and management to engage in full and frank discussions regarding the terms of the policy/initiative. We are also proposing that joint labor-management ground rules be developed that would expedite discussion of the issues.

During the next week or so I will be contacting you as Chair of the Coalition to discuss this win-win approach. If the CCU or any of its individual members have any suggestions or response we would encourage you forward them to our office.

Mr. Paul Roller, Chair

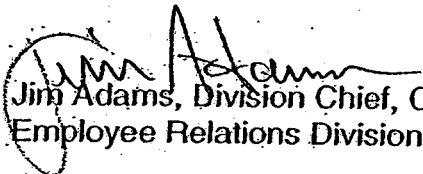
June 9, 2004

Page 3

I can be reached at (213) 974-2404 if you would like to discuss this matter further, or you may contact Don Washington, Assistant Division Chief, Employee Relations, at (213) 974-2497.

Sincerely,

DAVID E. JANSSEN
Chief Administrative Officer



Jim Adams, Division Chief, CAO
Employee Relations Division

DEJ:JA

DLW:mj

c: Each Member of the Coalition of County Unions